

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

APPROXIMATELY 32.68342694 BITCOIN  
(AND FUNDS DERIVED THEREFROM)  
FORMERLY HELD IN WALLET  
ADDRESS 1G3pyCCFENTp8EHANrG-  
BpmEKNobPqA5CLg, SEIZED FROM A  
BINANCE.COM EXCHANGE ACCOUNT  
ASSOCIATED WITH USER ID 395972026,

Defendant.

NO. CV23-2010

**VERIFIED COMPLAINT  
FOR FORFEITURE *IN REM***

COMES NOW the United States, by and through its undersigned counsel, and  
alleges:

**I. NATURE OF THE ACTION**

1. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(C) for forfeiture of cryptocurrency that constitutes or is derived from proceeds traceable to a violation of specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), including but not limited to wire fraud, 18 U.S.C. § 1343, or conspiracy to commit wire fraud, 18 U.S.C. § 1349.

2. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(A) for forfeiture of cryptocurrency that is involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and/or 1957, or any property traceable to such property.

## II. PLAINTIFF AND DEFENDANT *IN REM*

3. The plaintiff is the United States of America (the “Plaintiff” or “Government” or “United States”).

4. The defendant consists of approximately 32.68342694 Bitcoin (the Defendant Cryptocurrency), seized by the United States Secret Service (USSS) from an account at Binance associated with User ID 395972026 (the Subject Account).

5. The Subject Account was registered on January 26, 2022, using a telephone number ending x5174 and a specific email address provided by the user associated with the Subject Account (“Subject Account Email”). The initials of the user associated with the Subject Account are O.S.A.

6. The Defendant Cryptocurrency was formerly held in wallet address 1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg (the Subject Wallet or “1G3pyC”) in the Subject Account.

7. Pursuant to a forfeiture seizure warrant issued in the Western District of Washington, Cause No. MC23-062, and executed on August 4, 2023, the USSS took custody of the Defendant Cryptocurrency on or about October 2, 2023, and it remains in that agency’s custody.

8. According to [www.blockchain.com](http://www.blockchain.com), on October 2, 2023, one BTC was equal to approximately \$27,505.30 United States dollars. Therefore, on the date of seizure, 32.68342694 BTC would convert to approximately \$898,975 in United States currency. The value of cryptocurrency fluctuates and at any given time may be more or less than this estimate.

//

### III. JURISDICTION AND VENUE

9. This Court has jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345 and has jurisdiction over an action for forfeiture under 28 U.S.C. § 1355(a) and (b).

10. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because the acts or omissions giving rise to the forfeiture occurred in this district.

11. Pursuant to 18 U.S.C. § 981(f), all right, title, and interest in the Defendant Cryptocurrency vests in the United States at the time of the acts giving rise to the forfeiture.

12. Pursuant to Supplemental Rule G(2)(f), facts in support of a reasonable belief that the United States will be able to meet its burden of proof at trial are as follows and have been verified by the attached Verification of USSS Special Agent Paul Vanderwulp.

13. As provided in Supplemental Rule G(3)(b)(i), the Clerk of Court is required to issue a warrant to arrest the Defendant Cryptocurrency if it is in the government's possession, custody, or control. As such, the Court will have *in rem* jurisdiction over the Defendant Cryptocurrency when the accompanying Warrant of Arrest *In Rem* is issued, executed, and returned to the Court.

### IV. SUMMARY OF BASES FOR FORFEITURE

14. The United States alleges that the Defendant Cryptocurrency was involved in transactions and attempted transactions in violation of 18 U.S.C. §§ 1956 and 1957 (Money Laundering) and 1956(h) (Conspiracy to Commit Money Laundering) and constitutes, or was derived from, proceeds traceable to violations of 18 U.S.C. §§ 1343 (Wire Fraud) and 1349 (Conspiracy to Commit Wire Fraud). The Defendant Cryptocurrency is, therefore, subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C).

1           15.    The Defendant Cryptocurrency contains the remnants of funds swindled  
2 from victims, including victims in the Western District of Washington, through the  
3 course of a Business Email Compromise wire fraud scheme. These funds were  
4 subsequently laundered through a web of financial accounts and cryptocurrency wallet  
5 addresses before coming to rest in the Subject Account.

6           16.    Some of the conspirators, including D.W.B., D.B.R., M.A.L., A.L., S.W.,  
7 P.H., M.K., E.S., L.S., and K.D.W.<sup>1</sup> opened financial accounts at Wells Fargo Bank,  
8 N.A.; Bank of America, N.A.; JPMorgan Chase Bank, N.A., ACU, and UCB, bearing the  
9 names of what appeared to be legitimate real estate businesses, including The Payoff  
10 Service LLC; The Payoff Collection LLC; AKL Development LLC; Payoff Clearing  
11 Account; Payoff Service Account; and Payoff Processing Fund.

12           17.    The conspirators used these multiple financial accounts to facilitate the  
13 fraud and to conceal and disguise the source and destination of the illicitly procured funds  
14 by using multiple techniques, including instructing victims to wire funds to accounts at  
15 different financial institutions, with different entity names, and controlled by different  
16 conspirators; rapidly moving funds from the original gaining accounts to other accounts  
17 they controlled; converting the funds to personal checks and cashier's checks which were  
18 deposited to different accounts; withdrawing funds in cash; converting funds into virtual  
19 currency; transferring that virtual currency through a maze of wallet addresses; and  
20 comingling their fraud proceeds. Ultimately, though they traveled different paths, funds  
21 from multiple victims arrived at the same destination.

22           18.    Investigators have traced approximately 10.69 BTC derived from proceeds  
23 defrauded from four identified victims from the initial fraudulent wire transfers, through  
24 a series of financial accounts at multiple financial institutions, cash withdrawals, checks,  
25 purchases of cryptocurrency using wire transfers and cash purchases through  
26 \_\_\_\_\_

27 <sup>1</sup> Conspirators other than the individual associated with the Subject Wallet in the Subject Account are identified in this Complaint using their initials.

1 cryptocurrency kiosks, and transactions on the blockchain, into the Subject Wallet in the  
2 Subject Account, from which the Defendant Cryptocurrency was seized.

### 3 **V. PURPOSE OF FORFEITURE**

4 19. The purpose of this forfeiture action *in rem* is two-fold. First, forfeiture of  
5 the Defendant Cryptocurrency provides a means for the United States to help victims of  
6 the fraud scheme recover their funds. Second, forfeiture deters criminal activity by  
7 forfeiting and vesting title of the Defendant Cryptocurrency with the United States so that  
8 criminals do not maintain the fruits of crime and do not keep property that facilitated or  
9 was involved in crime.

### 10 **VI. THE LAW**

11 20. Pursuant to 18 U.S.C. § 1343, it is unlawful to devise or intend “to devise  
12 any scheme or artifice to defraud, or for obtaining money or property by means of false  
13 or fraudulent pretenses, representations, or promises, transmit[] or cause[] to be  
14 transmitted by means of wire, radio, or television communication in interstate or foreign  
15 commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing  
16 such scheme or artifice. . . .”

17 21. Pursuant to 18 U.S.C. § 1349, it is unlawful to attempt or conspire to  
18 commit a violation of 18 U.S.C. § 1343.

19 22. Pursuant to 18 U.S.C. § 981(a)(1)(A), “[a]ny property, real or personal,  
20 involved in a transaction or attempted transaction in violation of [a federal money  
21 laundering offense, 18 U.S.C. § 1956], or any property traceable to such property” is  
22 subject to forfeiture to the United States.

23 23. Pursuant to 18 U.S.C. § 981(a)(1)(C), “[a]ny property, real or personal,  
24 which constitutes or is derived from proceeds traceable to a violation of . . . any offense  
25 constituting a ‘specified unlawful activity’ (as defined in section 1956(c)(7) of this title),  
26 or a conspiracy to commit such offense” is subject to forfeiture to the United States.

24. Pursuant to 18 U.S.C. §1956(a)(1), it is unlawful to knowingly conduct or attempt to conduct a “financial transaction” with proceeds from “specified unlawful activity” (SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds, evade reporting requirements, or evade taxes. 18 U.S.C. § 1956(h) prohibits conspiracies to commit money laundering.

25. Pursuant to 18 U.S.C. §1956(a)(1), it is unlawful to knowingly engage or attempt to engage in a “monetary transaction” in property of a value greater than \$10,000 which is derived from “specified unlawful activity.” 18 U.S.C. § 1956(h) prohibits conspiracies to commit money laundering.

26. Pursuant to 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)(B), the offenses of wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349, constitute specific unlawful activity.

## **VII. BACKGROUND ON BUSINESS EMAIL COMPROMISE SCHEMES**

27. Business Email Compromise (“BEC”) schemes generally involve deceiving businesses to induct them to initiate large wire transfers from the business’ accounts to those controlled by the criminal organization or individual.

28. Since 2013, the Federal Bureau of Investigation (FBI) has tracked the emergence of BEC schemes worldwide. The criminal enterprises that perpetuate these schemes have targeted companies and organizations in every U.S. state and in more than 100 countries around the world. The losses caused by BEC schemes are in the billions of dollars and climbing.

29. The victims of BEC schemes range from small businesses to large corporations. Perpetrators will typically monitor and study their selected victims using social engineering techniques prior to initiating the BEC scheme. In many cases, the perpetrators can accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment.

30. As with many computer or internet facilitated financial crimes, the perpetrators of BEC schemes are increasingly using “money mules” to cash out the proceeds of their schemes and move the money to offshore accounts controlled by the operators of the schemes. “Money mules” are those hired by cybercrime rings to move the proceeds of financially motivated cybercrimes from the target country to the perpetrator’s home country. The money mules are often not directly involved in the attack against the victim of the BEC scheme and are only responsible for receiving and laundering the funds. In recent years, however, law enforcement has encountered professional money mules who repeatedly engage in these types of transactions fully aware of the criminal nature of their activities. In addition, cybercrime rings have begun to develop organized groups of money mules and money mule services that are offered to other criminal organizations for a fee.

31. The FBI has noted some of the following characteristics of BEC complaints:

a. Businesses and associated personnel using open-source email accounts are predominately targeted;

b. Individuals responsible for handling wire transfers within a specific business are targeted;

c. Spoofed emails closely mimic a legitimate email request;

d. Fraudulent email requests for a wire transfer are well-worded, specific to the business being victimized, and do not raise suspicions about the legitimacy of the request; and

e. The amount of the fraudulent wire transfer request is business-specific, so dollar amounts requested are similar to normal business transaction amounts to avoid raising suspicion.

//

//



# VIII. BACKGROUND ON DIGITAL OR VIRTUAL CURRENCY

32. Virtual or Digital Currency: Digital currency (also known as cryptocurrency or virtual currency)<sup>2</sup> is generally defined as an electronic-source unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.<sup>3</sup> Digital currency is not issued by any government or bank (in contrast to fiat currency) and is, instead, generated and controlled through computer software operating on a decentralized peer-to-peer network. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud based servers.

33. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, it is also often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership, or control of illegally obtained criminal proceeds. Bitcoin and Ethereum are some of the most commonly used and well-known digital currencies.

34. Perpetrators of fraud will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when transferred into a cryptocurrency exchange. The number of hops in the transactions is a strong indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

<sup>2</sup> For purposes of this Complaint, the terms “digital currency,” “cryptocurrency,” and “virtual currency” are used interchangeably and address the same concept.

<sup>3</sup> Fiat currency is currency issued and regulated by a government, such as the U.S. Dollar, Euro, or Japanese Yen.



35. Perpetrators of fraud often launder proceeds of their fraud schemes through several virtual wallet addresses or accounts before transferring the proceeds to those individuals near or at the top of the criminal organization's hierarchy.

36. Virtual or Digital Currency Addresses: Digital or virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

37. Private Key: Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

38. Address Owner: The identity of an address owner is generally considered to pseudonymous (unless the owner opts to make the information publicly available), often law enforcement and currency exchanges can use the blockchain to identify the owner of a particular address and trace fraud proceeds from victims to one or more exchanges or wallets. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

39. Blockchain: Many virtual currencies publicly record their transactions on what is referred to as the "blockchain."<sup>4</sup> The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every

---

<sup>4</sup> Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

1 transaction and all the known balances for each virtual currency address. There are  
2 different blockchains for different types of virtual currencies. Investigators can follow or  
3 “trace” funds on public blockchains, a practice known as “blockchain analysis.”

4 40. Blockchain Analysis: It is virtually impossible to look at a single  
5 transaction on a blockchain and immediately ascertain the identity of the individual  
6 behind the transaction. That is because blockchain data generally consist only of  
7 alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the  
8 identity of the owner of an address by analyzing blockchain data to figure out whether  
9 that same individual is connected to other relevant addresses on the blockchain. To  
10 analyze blockchain data, law enforcement can use blockchain explorers as well as  
11 commercial services offered by blockchain-analysis companies. These companies  
12 analyze virtual currency blockchains and attempt to identify the individuals or groups  
13 involved in transactions. Through numerous unrelated investigations, law enforcement  
14 has found the information provided by these tools to be reliable.

15 41. Virtual Currency Wallet: A virtual currency wallet is a software application  
16 that interfaces with the virtual currency’s specific blockchain and generates and stores a  
17 user’s addresses and private keys. A virtual currency wallet also allows users to send and  
18 receive virtual currencies. Multiple addresses can be stored in a wallet. Even though the  
19 public address of those engaging in digital currency transactions are recorded on the  
20 public ledger, the true identities of the individuals or entities behind the public address  
21 are not recorded. If a real individual or entity is linked to a public address, however, it  
22 may be possible to determine what transactions were conducted by that individual or  
23 entity. Therefore, digital transactions are often described as “pseudonymous,” meaning  
24 they are partially anonymous. Most individuals are identified when they use a digital  
25 currency exchange to make a transaction between digital currency and fiat currency, or  
26 through digital currency exchangers that voluntarily or through legal order, cooperate  
27 with law enforcement.

42. Virtual Currency Exchange: A digital or virtual currency exchange (an “exchange”) is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Many exchanges are located outside the boundaries of the United States to avoid regulation and legal requirements. One of the largest and most popular exchanges is Binance.

43. Because exchanges act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., “know your customer” or “KYC” checks) and to have anti-money laundering programs in place.

44. Peel chain: Peel chain is a technique used to launder large amounts of illegally obtained cryptocurrency by funding a long series of small transactions. In other words, a small amount is “peeled” from a person’s holdings in a low-value transfer again and again, often through an exchange where it can be converted to fiat currency.

#### **IX. SCHEME TO DEFRAUD AND FINANCIAL TRACING**

45. This case involves a Business Email Compromise (BEC) wire fraud scheme, perpetrated on victims across the United States, including in the Western District of Washington. The wire fraud scheme involved compromising email and facsimile systems of multiple businesses and using those compromised systems without authority to fraudulently obtain funds intended to be used in legitimate real estate transactions. The conspirators impersonated personnel or customers of the victim businesses and directed them to initiate wire transfers to bank accounts controlled by the conspirators. The conspirators engaged in layered financial transactions designed, in whole or in part, to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Many of these transactions involved more than \$10,000 of proceeds from the wire fraud scheme.

46. Proceeds defrauded from at least four identified victims of the wire fraud scheme flowed into and through financial accounts controlled by the conspirators and were ultimately traced to the Subject Wallet (“1G3pyC”) in the Subject Account, where they were seized. Several victims sent wire transfers to multiple financial accounts, bearing different names, and controlled by different conspirators working together. For example, one victim sent wire transfers to four different banks, directed to four business names, and controlled by four conspirators:

Date	Amount	Financial Account	Business Name	Conspirator
2-22-2022	\$60,652.81	JPMorgan Chase x7218	The Payoff Collection LLC	M.K.
3-8-2022	\$60,629.30	Wells Fargo x7903	Payoff Clearing Account	S.W.
3-24-2022	\$107,149.96	Wells Fargo x7903	Payoff Clearing Account	S.W.
3-25-2022	\$43,419.17	Bank of America x3839	Payoff Clearing Account	S.W.
4-4-2022	\$99,502.49	JPMorgan Chase x5767	The Payoff Express LLC	E.S.
4-6-2022	\$159,190.19	Wells Fargo 8183	Payoff Service Account	P.H.

47. The USSS initiated this investigation after receiving a fraud report from a victim business located in Seattle, Washington, which lost approximately \$1,192,339.33 after falling victim to this BEC wire fraud scheme. Subsequent investigation identified more than ten additional victim businesses of this BEC wire fraud scheme and at least \$4 million dollars of fraudulently obtained criminal proceeds.

48. Based on the Know Your Customer (“KYC”) information provided to Binance, the Subject Account was registered from Nigeria.

49. This Complaint does not include all of the financial analysis of fiat and virtual currency performed, but focuses on the tracing of specific funds from victims into

1 the Subject Account, to demonstrate the concerted efforts to launder and obfuscate the  
2 flow of victim funds into the Subject Account. Financial account numbers and  
3 cryptocurrency addresses are truncated throughout this Complaint.

4 50. Identified victims of this BEC fraud scheme include:

5 a. Victim 1 is a real estate closing business located in Seattle,  
6 Washington, which incurred a total loss of approximately \$1,192,339.33. Victims 1 – 5  
7 are all victims of the same BEC wire fraud scheme conducted by these conspirators.  
8 Fraud proceeds obtained from Victim 1 have not been traced to the Subject Account, but  
9 have been traced to financial accounts of one or more conspirators involved in the  
10 scheme who also received victim funds that have been traced to the Subject Account. The  
11 imposter email addresses used to compromise the eFax systems of Victims 1, 2, and 3 are  
12 connected by computer cookies.

13 b. Victim 2 is a law firm located in Florida, which incurred a total loss  
14 of approximately \$530,543.92.

15 c. Victim 3 is a law firm located in Florida, which incurred a total loss  
16 of approximately \$425,572.59.

17 d. Victim 4 is a title company located in Florida, which incurred a total  
18 loss of approximately \$302,683.25.

19 e. Victim 5 is a title company located in Florida, which incurred a total  
20 loss of approximately \$198,888.07.

21 Proceeds of the BEC fraud scheme obtained from Victim 2, Victim 3, Victim 4, and  
22 Victim 5 have been traced to the Subject Wallet in the Subject Account, from which the  
23 Defendant Cryptocurrency was seized. Graphic images depicting this tracing are  
24 embedded herein and attached as Exhibits A, B, and C. Exhibit D depicts tracing from  
25 each of these four victims into the Subject Account.

26 //

### ***Conspirator Financial Accounts***

51. Some of the conspirators opened numerous accounts at financial institutions, using the names of individuals, entities, or both. The primary accounts involved in tracing funds defrauded from Victims 1-5 appear in the table below, with reference monikers. The names of individual conspirators are abbreviated to initials.

Financial Institution	Account Ending	Name	Moniker
Wells Fargo	-5021	D.W.B. dba Payoff Processing Fund	WF Account 1
Wells Fargo	-6202	D.B.R. dba Payoff Service Processing	WF Account 2
Wells Fargo	-7903	S.W. dba Payoff Clearing Account	WF Account 3
Wells Fargo	-8183	P.H. dba Payoff Service Account	WF Account 4
Bank of America	-9274	M.A.L. Sole Prop dba Payoff Clearing Account	BOA Account 1
Bank of America	-5686-	AKL Development LLC	BOA Account 2
Bank of America	-7812	DBA Payoff Service Processing D.B.R. Sole Prop	BOA Account 3
Bank of America	-3839	S.W. Sole Prop dba Payoff Clearing Account	BOA Account 4
Bank of America	-4988	Payoff Service Account	BOA Account 5
JPMorgan Chase	-1857	D.W.B. dba Payoff Processing Fund	JPMC Account 1
JPMorgan Chase	-7218	M.K. dba The Payoff Collection LLC	JPMC Account 2
Advantis Credit Union	-3002	L.S.	ACU Account 1
United Community Bank	-4746	K.D.W. Payoff Account Service	UCB Account 1
United Community Bank	-4754	K.D.W. (check)	UCB Account 2
Bank of the West	-3405	M.K.	BOTW Account 1
Bank of the West	-3447	M.K.	BOTW Account 2

### ***Victim 1***

52. On or around February 14, 2023, one or more conspirators successfully compromised Victim 1's eFax.com account, likely through a spear phishing email. Victim 1 used its eFax account to digitally send and receive faxes. One or more conspirators removed Victim 1's legitimate email address from the fax forwarding preferences to prevent faxes from arriving in Victim 1's email mailbox. One or more conspirators then added an email address they controlled ("Imposter Email 1"), to the fax

1 forwarding preferences, which allowed them to monitor eFax communications intended  
2 for Victim 1. The conspirators used the information they obtained from this subterfuge to  
3 review legitimate faxes to Victim 1's closing team and learn Victim 1's business  
4 practices. The conspirators used this information without authority to impersonate Victim  
5 1's personnel and customers, and issued instructions to other Victim 1 employees,  
6 directing them to initiate wire transfers to bank accounts controlled by the conspirators.

7 53. The conspirators used Imposter Email 1 address to monitor Victim 1's eFax  
8 account for approximately one month. During that period, Imposter Email 1 intercepted  
9 at least eight communications that were intended for Victim 1. Many of these  
10 communications contained wire transfer details, customer names, and other bank  
11 information related to financial transactions for escrow and estate closing proceedings.

12 54. After compromising Victim 1's eFax account, one or more conspirators  
13 sent Victim 1 at least two wire instruction sheets that were forgeries, resulting in  
14 fraudulent wire transfers from Victim 1's corporate account at Capital Bank MD, totaling  
15 \$1,192,339.33. The forged wire instructions purported to be mortgage payoff instructions  
16 in anticipated monetary amounts to be sent by wire transfer to anticipated financial  
17 institutions.

18 ***Wire 1***

19 55. On March 13, 2023, based on fraudulent wire transfer instructions, Victim  
20 1 sent a wire transfer in the amount of \$681,146.02 from Victim 1's corporate account at  
21 Capital Bank MD in the District of Washington to a Wells Fargo Bank, N.A. account  
22 ending -5021, located in Cedar Park, Texas (Wire 1).

23 a. The receiving account is held in the name of [D.W.B.] dba Payoff  
24 Processing Fund (WF Account 1) and was opened on November 28, 2022. Account  
25 opening documents identify D.W.B. as the sole owner of the business.

26 b. Immediately prior to receiving Wire 1, WF Account 1 had a balance  
27 of \$30.00.



c. One or more conspirators then used \$100,000 of the fraud proceeds involved in Wire 1 to fund a personal check in the amount of \$100,000, purportedly signed by D.W.B. This check was subsequently deposited to a JP Morgan Chase Bank, N.A. account ending -1857, held in the name of [D.W.B.] dba Payoff Processing Fund (JPMC Account 1). The balance in JPMC Account 1 prior to the deposit of this check was \$5.00.

**Wire 2**

56. On March 15, 2023, based on fraudulent wire transfer instructions, Victim 1 sent a wire transfer in the amount of \$511,193.31 from Victim 1's corporate account at Capital Bank MD in the District of Washington to a Wells Fargo Bank, N.A. account ending -6202, located in Harris County, Texas (Wire 2).

a. The receiving account is held in the name of [D.B.R.] dba Payoff Service Processing (WF Account 2) and was opened on October 26, 2022.

b. Immediately prior to receiving the wire from Victim 1, WF Account 2 had a balance of \$41.62.

57. One or more conspirators then used \$477,500 of fraud proceeds involved in Wire 2 to purchase four cashier's checks.

a. On March 17, 2023, a cashier's check in the amount of \$150,000 was deposited using an automated teller machine (ATM) into a Bank of America, N.A. account ending -9274. This account is held in the name of [M.A.L.] Sole Prop DBA Payoff Clearing Account (BOA Account 1) and was opened on September 20, 2022. The face of the cashier's check reflected D.B.R. as remitter and M.A.L. as payee.

b. On March 17, 2023, a cashier's check in the amount of \$150,000 was deposited by ATM into a Bank of America, N.A. account ending -5686. The receiving account is held in the name of AKL Development, with A.L. identified as managing member (BOA Account 2) and was opened on November 29, 2022. The face of the cashier's check reflects D.B.R. as remitter and A.L. as payee.

1           c.       On March 16, 2023, a cashier's check in the amount of \$150,000  
2 was credited to a Bank of America, N.A. account ending -7812. This account is held in  
3 the name of DBA Payoff Service Processing [D.B.R.] Sole Prop (BOA Account 3) and  
4 was opened on October 26, 2022. The face of the cashier's check reflects D.B.R. as both  
5 remitter and payee.

6           d.       On March 16, 2023, a cashier's check number in the amount of  
7 \$27,500 was provided to a bank teller for deposit into BOA Account 3. The face of the  
8 cashier's check reflects D.B.R. as both remitter and payee.

9       58.       On or about March 31, 2023, Magistrate Judge Mary Alice Theiler  
10 authorized seizure of the fraud proceeds from the wires sent by Victim 1 to BOA  
11 Accounts 1, 2, and 3. *See* Western District of Washington Cause No. MC23-027-MAT.

12       59.       On or about April 21, 2023, Magistrate Judge S. Kate Vaughn authorized  
13 seizure of the fraud proceeds from the wires sent by Victim 1 to JPMC Account 1. *See*  
14 Western District of Washington Cause No. MC23-035.

15 ***Communication with Conspirator S.W.***

16       60.       On or about April 12, 2023, shortly after funds were seized from BOA  
17 Accounts 1, 2, and 3, an individual identifying herself as "S.W." called a USSS Special  
18 Agent to inquire about the seized funds. S.W. said that she was the mother of A.L.,  
19 denied he was involved in any wrongdoing, and asked why he was targeted but the "other  
20 two" were not, without disclosing the names of the "other two."

21       61.       About a week later, on or about April 20, 2023, S.W. again called the same  
22 USSS Special Agent and admitted that she was paid to move money for an individual  
23 named W.W. and that she referred D.B.R. to W.W. for the same type of job. S.W.  
24 explained that D.B.R. and her two sons, M.A.L. and A.L., worked on the "[Victim 1]  
25 job" under her supervision because she was "training" them. Significantly, only the  
26 perpetrators of the fraud would have known that Victim 1 was the victim of the fraud  
27 scheme from which the proceeds were seized from the Bank of America accounts and

1 that D.B.R., M.A.L., and A.L. were involved because this was not publicly available  
2 information. S.W. said that W.W., D.B.R. and the other individuals communicated with  
3 each other using email.

4 62. Subsequently, on or about April 20, 2023, S.W. contacted the same USSS  
5 Special Agent to provide contact information for J.K., whom she claimed would validate  
6 that she was legitimately “employed” when she helped move funds, including for the  
7 Victim 1 transactions (Wire 1 and Wire 2). S.W. also said that she worked for at least two  
8 different people that she met online and that she was directed by these individuals to help  
9 move money.

10 63. During this investigation, the USSS became aware that S.W. had an active  
11 warrant for her arrest from the Fayette County (Georgia) Sheriff’s Office arising out of  
12 her involvement in a BEC scam that defrauded Victim 2, Victim 3, and other law firms  
13 that conduct real estate closing transactions. Upon her arrest by Georgia law enforcement,  
14 S.W. described several individuals that she referred to as her “handlers” as speaking with  
15 an “African” accent. M.A.L. and A.L. also informed law enforcement that they had  
16 spoken by telephone with a male who had an “African” accent.

17 ***Victim 2***

18 64. Victim 2 represents clients selling residential homes. In or around April  
19 2022, Victim 2 was notified by three different individuals that the payoff for their home  
20 loans had not been received even though Victim 2 thought it had wired the funds as  
21 instructed.

22 65. A subsequent investigation revealed that Victim 2’s eFax.com account had  
23 been compromised in or around December 2021. One or more conspirators removed  
24 Victim 2’s email address for the eFax account and replaced it with an email address they  
25 controlled, Imposter Email 2, so they could monitor legitimate incoming communications  
26 to Victim 2. As a result of this subterfuge, the conspirators obtained faxes with wiring  
27 instructions that Victim 2 was expecting and altered those wiring instructions. One or

1 more conspirators then removed Imposter Email 2 from Victim 2's compromised eFax  
2 account, replaced it with the true Victim 2 email address, and faxed the fraudulent wiring  
3 instructions to Victim 2's eFax account.

4 66. Through this scheme, the conspirators duped Victim 2 into sending at least  
5 six wires transfers totaling over \$530,000 into accounts in the custody and control of the  
6 conspirators. At least \$322,198.43 of these proceeds was then transferred into other  
7 financial accounts controlled by one or more of the conspirators. Victim 2 sent at least  
8 \$211,198.43 directly to S.W.'s accounts at Bank of America and Wells Fargo. Victim 2  
9 sent a third wire transfer to a funnel account held by P.H., who then transferred  
10 approximately \$111,000 of those funds to one of S.W.'s accounts at Bank of America.

11 a. On or about March 8, 2022, based on fraudulent wire transfer  
12 instructions, Victim 2 wired \$60,629.30 to a Wells Fargo account ending -7903. This  
13 account is held in the name of [S.W.], doing business as Payoff Clearing Account (WF  
14 Account 3), and was opened on January 19, 2022.

15 b. On or about March 24, 2022, based on fraudulent wire transfer  
16 instructions, Victim 2 sent a second wire transfer of \$107,149.96 to WF Account 3.

17 c. On or about March 25, 2022, based on fraudulent wire transfer  
18 instructions, Victim 2 sent a wire transfer of \$43,419.17 to a Bank of America account  
19 ending -3839, in the name of [S.W.] Sole Prop, doing business as Payoff Clearing  
20 Account (BOA Account 4).

21 d. On or about April 6, 2022, based on fraudulent wire transfer  
22 instructions, Victim 2 wired \$159,190.19 to a Wells Fargo account ending -8183. The  
23 receiving account was held in the name of [P.H.] (WF Account 4). Approximately one  
24 day later, P.H. rapidly depleted the funds from WF Account 4, including by sending  
25 \$111,000 of the funds to WF Account 3.

26 //

27 //

**Victim 3**

67. One or more conspirators also compromised the eFax account of Victim 3, which incurred losses totaling \$425,572.59. Using the same *modus operandi*, the conspirators replaced Victim 3's true email address with Imposter Email 2, the same email address used in the compromise of Victim 2's eFax system, then sent fraudulent wire transfer instructions to Victim 3.

68. On or about March 25, 2022, based on fraudulent wire instructions, Victim 3 wired \$288,324.60 to WF Account 3.

**Further tracing of Proceeds Defrauded from Victim 2 and Victim 3**

69. As described above, BEC fraud scheme Victims 2 and 3 sent wires based on fraudulent wire transfer instructions to bank accounts at Wells Fargo and Bank of America, in the name of or controlled by conspirators, including S.W. (WF Account 3).

70. Victims 2 and 3 wired a total of \$456,103.86 directly to WF Account 3. Victim 2 wired an additional \$159,190.19 to WF Account 4; \$111,000 of those funds were then wired from WF Account 4 to WF Account 3.

71. After each wire was deposited to WF Account 3, one or more conspirators conducted financial transactions to remove the proceeds from that account, primarily using cash withdrawals and wire transfers to BOA Account 4.

a. March 3, 2022 Victim 2 wire to WF Account 3 (\$60,629.30):

(1) WF Account 3 had a balance immediately prior to the \$60,629.30 wire of \$3.00.

(2) On or about March 9, 2022, S.W. made a cash withdrawal of \$20,000, wired \$37,000.00 from WF Account 3 to BOA Account 4, and sent a peer-to-peer payment using Zelle to A.L., among other transactions.

b. March 24, 2022 Victim 2 wire to WF Account 3 (\$107,149.96):

(1) WF Account 3 had a balance immediately prior to the \$107,149.96 wire from Victim 2 of \$62.12.

(2) The only deposit to WF Account 3 between the first two wires from Victim 2 was a \$30 online transfer from another S.W. account.

c. March 25, 2022 Victim 3 wire to WF Account 3 (\$288,324):

(1) WF Account 3 had a balance immediately prior to the \$288,324 wire from Victim 3 of \$105,197.08, all of which was proceeds from the wire transfers from Victim 2.

(2) On or about March 25, 2022, S.W. made a cash withdrawal of \$20,000 from WF Account 3 and a wire transfer of \$81,000.00 from WF Account 3 to BOA Account 4.

(3) On or about March 28, 2022, S.W. made a wire transfer of \$200,000 to BOA Account 4, transferred approximately \$18,850 to a Wells Fargo account ending -8497 that she holds with A.L., and a few other transactions, leaving a balance in BOA Account 4 of \$59,006.68, all of which was proceeds from the wire transfers from Victims 2 and 3.

(4) On or about March 29, 2022, S.W. withdrew cash of \$20,000.

(5) On or about March 31, 2022, S.W. withdrew cash of \$25,000.

(6) WF Account 3 had a closing balance on March 31, 2022 of \$14,006.68, all of which was funds remaining from the wire transfers of Victims 2 and 3.

d. Between March 9, 2022 and March 31, 2022, S.W. conducted multiple cash withdrawals from WF Account 3, totaling \$85,000.00.

e. April 7, 2023 wire from P.H. of Victim 2 Funds (\$111,000):

(1) Prior to the \$111,000 wire from P.H.'s WF Account 4, the balance in WF Account 3 was \$22.32.

(2) On or about April 8, 2022, S.W. made a \$25,000 cash withdrawal and transferred \$40,000 to BOA Account 4.

(3) On or about April 11, 2022, S.W. made a \$30,000 cash withdrawal from WF Account 3 and a \$5,000 purchase, using a linked debit card, leaving a balance in WF Account 3 of \$77.32.

72. BOA Account 4 received five deposits in March 2022:

a. Three deposits were transfers from WF Account 4 consisting of proceeds defrauded from Victims 2 and 3, as set forth above.

b. One was a transfer directly from Victim 2, which was also proceeds.

c. One was a wire transfer in the amount of \$67,253.40 from First Horizon Bank, described as “Pay off loan #417264900”, which also appears to be proceeds of the BEC wire fraud scheme. The sending entity is Orion Title & Escrow LLC.

d. Prior to the first deposit of March 1, 2022, the balance on BOA Account 4 was \$1,000.

Date	Amount	Sending Account	Destination Moniker	Destination Account Number
3-1-2022	\$67,253.40	First Horizon	BOA Account 4	BOA-3839
3-9-2022	\$37,000.00	WF Account 3	BOA Account 4	BOA-3839
3-25-2022	\$81,000.00	WF Account 3	BOA Account 4	BOA-3839
3-25-2022	\$43,419.17	Victim 2	BOA Account 4	BOA-3839
3-28-2022	\$200,000.00	WF Account 3	BOA Account 4	BOA-3839
Total:	\$428,672.57			

e. S.W. also made an additional wire transfer from WF Account 3 to BOA Account 4 of \$40,000 on April 8, 2022, which consisted of proceeds defrauded from Victim 2.

f. BOA Account 4 received three other deposits during this period, totaling \$2,320, from a Zelle account associated with S.W.

g. After the proceeds defrauded from Victims 2 and 3 were deposited into BOA Account 4, one or more conspirators made cash withdrawals from that account, totaling approximately \$259,731 between March 10 and April 8, 2022.



73. Between March 3, 2022 and April 8, 2022, approximately \$658,713.12 of fraud proceeds from Victims 2 and 3 were deposited into accounts controlled by these conspirators and approximately \$295,500 of these fraud proceeds were withdrawn from WF Account 3 and BOA Account 4 in cash.

74. The flow of proceeds from initial wire transfers from Victims 2 and 3, to and through conspirator financial accounts WF Account 3, WF Account 4, and BOA Account 4 is depicted in the table below. Victim 2 and 3 wires are shaded purple. Wires between conspirator accounts are shaded orange. Cash withdrawals are shaded green:

DATE	ACCOUNT NUMBER	MONIKER	CREDIT AMOUNT	DEBIT AMOUNT	TYPE
3/8/2022	WF-7903	WF Account 3	\$60,629.30		Wire from Victim 2
3/9/2022	WF-7903	WF Account 3		\$20,000.00	Cash Withdrawal
3/9/2022	WF-7903	WF Account 3		\$37,000.00	Wire to BOA Account 4
3/9/2022	BOA-3839	BOA Account 4	\$37,000.00		Wire from WF Account 3
3/10/2022	BOA-3839	BOA Account 4		\$15,000.00	Cash Withdrawal
3/11/2022	BOA-3839	BOA Account 4		\$22,000.00	Cash Withdrawal
3-24-2022	WF-7903	WF Account 3	\$107,149.96		Wire from Victim 2
3/25/2022	WF-7903	WF Account 3	\$288,324.60		Wire from Victim 3
3-25-2022	WF-7903	WF Account 3		\$20,000.00	Cash Withdrawal
3-25-2022	WF-7903	WF Account 3		\$81,000.00	Wire to BOA Account 4
3/25/2022	BOA-3839	BOA Account 4	\$81,000.00		Wire from WF Account 3
3/25/2022	BOA-3839	BOA Account 4	\$43,419.17		Wire from Victim 2
3/28/2022	BOA-3839	BOA Account 4		\$38,500.00	Cash Withdrawal
3/28/2022	BOA-3839	BOA Account 4		\$30,000.00	Cash Withdrawal
3/28/2022	WF-7903	WF Account 3		\$200,000.00	Wire to BOA Account 4
3/28/2022	BOA-3839	BOA Account 4	\$200,000.00		Wire from WF Account 3
3/29/2022	WF-7903	WF Account 3		\$20,000.00	Cash Withdrawal
3/29/2022	BOA-3839	BOA Account 4		\$15,000.00	Cash Withdrawal
3/29/2022	BOA-3839	BOA Account 4		\$10,000.00	Cash Withdrawal
3/30/2022	BOA-3839	BOA Account 4		\$10,000.00	Cash Withdrawal
3/31/2022	BOA-3839	BOA Account 4		\$20,000.00	Cash Withdrawal
3/31/2022	WF-7903	BOA Account 4		\$25,000.00	Cash Withdrawal
4/1/2022	BOA-3839	BOA Account 4		\$50,000.00	Cash Withdrawal
4/4/2022	BOA-3839	BOA Account 4		\$30,231.00	Cash Withdrawal
4/4/2022	BOA-3839	BOA Account 4		\$10,000.00	Cash Withdrawal
4/6/2022	WF-8183	WF Account 4	\$159,190.19		Wire from Victim 2
4-7-2022	WF-8183	WF Account 4		\$111,000.00	Wire to WF Account 3
4-7-2022	WF-8183	WF Account 4		\$40,000.00	Wire to WF Account 3

4-8-2022	WF-7903	WF Account 3	\$111,000.00		Wire from WF Account 4
4-8-2022	WF-7903	WF Account 3		\$40,000.00	Wire to BOA Account 4
4-8-2022	BOA-3839	BOA Account 4	\$40,000.00		Wire from WF Account 3
4-8-2022	BOA-3839	BOA Account 4		\$9,000.00	Cash Withdrawal

75. One or more conspirators then converted some of these fraud proceeds from fiat currency to virtual currency, using virtual currency ATMs operated by Bitcoin Depot and other vendors and wire transfers. Some of the purchased cryptocurrency has been traced to the Subject Wallet at the Subject Account.

#### ***S.W. Virtual Currency Purchases***

76. Between March 9, 2022 and March 29, 2022, S.W. deposited \$66,380.00 in cash into Bitcoin Depot ATMs for the purchase of virtual currency. The associated virtual currency, totaling 1.25817582 BTC, was deposited into three identified wallet addresses:

Transaction Date	Transaction Value [Bitcoin]	Receiving Wallet Address
3/9/2022 11:13	0.09633957	bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh
3/9/2022 11:18	0.0018947	bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh
3/10/2022 11:13	0.31649687	bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh
3/25/2022 13:03	0.28358918	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
3/26/2022 12:19	0.11853435	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
3/26/2022 12:28	0.00332022	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
3/28/2022 11:55	0.26297146	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
3/29/2022 14:59	0.17502947	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
<b>TOTAL:</b>	1.25817582	

Transaction Date	Transaction Value [Fiat]	Transaction Value [Bitcoin]	Receiving Wallet Address (Truncated)	Moniker
3/9/2022	\$4,900	0.09633957	bc1q9n	Wallet 1
3/9/2022	\$100	0.0018947	bc1q9n	Wallet 1
3/10/2022	\$14,900	0.31649687	bc1q9n	Wallet 1
3/25/2022	\$15,000	0.28358918	bc1qm3	Wallet 2
3/26/2022	\$6,300	0.11853435	bc1qm3	Wallet 2
3/26/2022	\$180	0.00332022	bc1qm3	Wallet 2
3/28/2022	\$15,000	0.26297146	bc1qm3	Wallet 2
3/29/2022	\$10,000	0.17502947	bc1qhl	Wallet 3
<b>TOTAL:</b>	\$66,380	1.25817582		

77. Between March 9, 2022 and March 10 2022, Wallet 1 (bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh or truncated as “bc1q9n”), shaded in the tables above in yellow, received virtual currency from three S.W. transactions, totaling approximately 0.41 BTC. On March 16, 2022, 0.41 BTC was combined with other deposits and a total of 1.47 BTC was sent to the Subject Wallet held in the Subject Account. 0.41 BTC of this transaction is proceeds of, or property derived from proceeds of, the wire fraud scheme and is traceable to the funds defrauded from Victim 2.

78. Between March 25, 2022 and March 28, 2022, Wallet 2 (bc1qm3h49m0mdzrda0rwkdly8vh04zv4wrt68zahe3 or truncated as “bc1qm3”), shaded in the table above in green, received virtual currency from four S.W. transactions, totaling approximately 0.67 BTC. On March 28, 2022, 0.67 BTC was combined with other deposits and a total of 1.29 BTC was sent to the Subject Wallet held in the Subject Account. 0.67 BTC of this transaction is proceeds of, or property derived from proceeds of, the wire fraud scheme and is traceable to the funds defrauded from Victims 2 and 3.

79. Wallet 3 (bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r or truncated as “bc1qhl”), shaded in the table above in blue, received 0.17 BTC from a S.W. transaction on March 29, 2022. On April 1, 2022, 0.17 BTC was combined with other deposits and a total of 1.93 BTC was sent to the Subject Wallet held in the Subject Account. 0.17 BTC of this transaction is proceeds of, or property derived from proceeds of, the wire fraud scheme and is traceable to the funds defrauded from Victims 2 and 3.

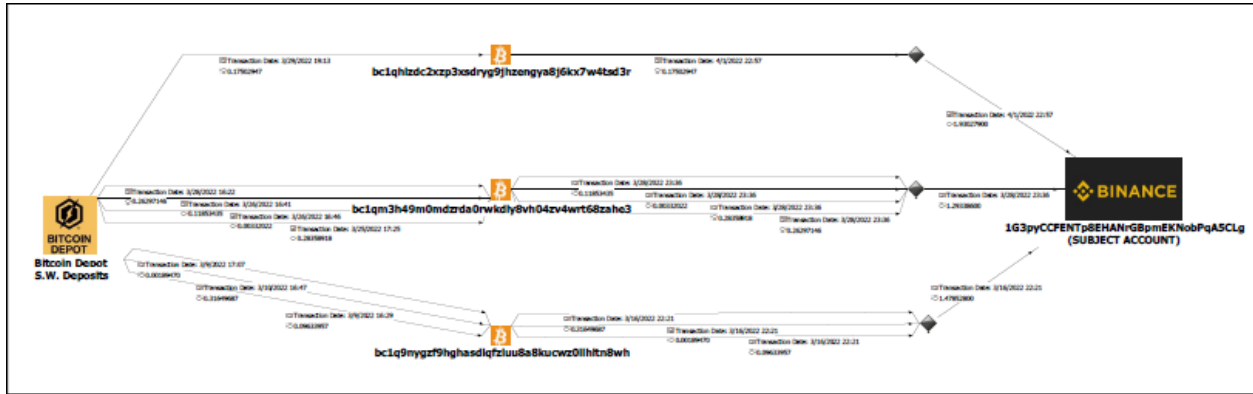
//

//

//

//

80. A visual representation of the tracing of these funds from the Bitcoin Depot ATM transactions conducted by S.W. to the Subject Wallet in the Subject Account is provided below, and is attached as Exhibit A:



81. During this period, S.W. also purchased virtual currency using other vendors, including LibertyX, RockItCoin, National Air of Texas.

a. Between March 28, 2022 and April 10, 2022, S.W. conducted at least 11 transactions with LibertyX, in which she purchased approximately 0.93993581 BTC for approximately \$46,850. S.W. sent this BTC to various wallet addresses, including approximately 0.13120063 BTC to Wallet 3.

Transaction Date	Transaction Value [Bitcoin]	Receiving Wallet Address
2022-03-28 14:16	0.09602031	3GjdrwhS9o9xUn4cw9MJePqRbXZBTR44aU
2022-03-30 12:11	0.09720147	3GjdrwhS9o9xUn4cw9MJePqRbXZBTR44aU
2022-03-31 18:25	0.09992026	3GjdrwhS9o9xUn4cw9MJePqRbXZBTR44aU
2022-04-01 14:07	0.09829505	3GjdrwhS9o9xUn4cw9MJePqRbXZBTR44aU
2022-04-02 12:34	0.09885833	bc1q6m7j8pwtf9s2s0ss5wrgt37697g78gt63qn6fs
2022-04-03 11:59	0.09856943	bc1q6m7j8pwtf9s2s0ss5wrgt37697g78gt63qn6fs
2022-04-04 11:28	0.10017514	3KJnzSmgd9e4cu5q4x5XSNXXNDsCHNZyKz
2022-04-05 10:43	0.01494602	bc1q35cakm3s5nalmdltl33z7ncxjw805r2zecdmgd
2022-04-08 12:23	0.10474917	3KJnzSmgd9e4cu5q4x5XSNXXNDsCHNZyKz
2022-04-09 14:33	0.10762963	bc1qhlzdc2x3p3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-10 11:14	0.02357100	bc1qhlzdc2x3p3xsdryg9jhzengya8j6kx7w4tsd3r
<b>TOTAL:</b>	<b>0.93993581</b>	

Transaction Date	Transaction Value [Fiat]	Transaction Value [Bitcoin]	Receiving Wallet Address (Truncated)	Moniker
2022-03-28 14:16	\$5,000	0.09602031	3Gjdrw	Wallet 4
2022-03-30 12:11	\$5,000	0.09720147	3Gjdrw	Wallet 4
2022-03-31 18:25	\$5,000	0.09992026	3Gjdrw	Wallet 4
2022-04-01 14:07	\$5,000	0.09829505	3Gjdrw	Wallet 4
2022-04-02 12:34	\$5,000	0.09885833	bc1q6m	
2022-04-03 11:59	\$5,000	0.09856943	bc1q6m	
2022-04-04 11:28	\$5,000	0.10017514	3KJnzS	
2022-04-05 10:43	\$750	0.01494602	bc1q35	
2022-04-08 12:23	\$5,000	0.10474917	3KJnzS	
2022-04-09 14:33	\$5,000	0.10762963	bc1qhl	Wallet 3
2022-04-10 11:14	\$1,100	0.02357100	bc1qhl	Wallet 3
<b>TOTAL:</b>	\$46,850	0.93993581		

b. Between March 25, 2022 and April 9, 2022, S.W. conducted at least 12 transactions with RockitCoin, in which she purchased approximately 2.34959885 BTC for approximately 0.93993581 BTC for approximately \$118,800. S.W. sent this BTC to various wallet addresses, including approximately 0.39980813 BTC to Wallet 2 (\$7,800) and approximately 1.84090157 to Wallet 3 (\$104,800).

Transaction Date	Transaction Value [Bitcoin]	Receiving Wallet Address
2022-03-25 12:23	0.09416196	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
2022-03-26 10:57	0.28285732	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
2022-03-28 11:41	0.02278885	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3
2022-03-28 12:03	0.10888915	3GjdrwhS9o9xUn4cw9MJEPqRbXZBTR44aU
2022-03-29 11:20	0.2602784	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-03-30 10:50	0.17670476	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-03-31 10:32	0.26801695	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-01 10:40	0.26820749	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-02 10:44	0.2706255	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-03 11:33	0.0180183	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-08 10:27	0.28455892	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-09 11:54	0.29449125	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
<b>TOTAL:</b>	2.34959885	

Transaction Date	Transaction Value [Fiat]	Transaction Value [Bitcoin]	Receiving Wallet Address [Truncated]	Moniker
2022-03-25 12:23	\$5,000	0.09416196	bc1qm3	Wallet 2
2022-03-26 10:57	\$1,500	0.28285732	bc1qm3	Wallet 2
2022-03-28 11:41	\$1,300	0.02278885	bc1qm3	Wallet 2
2022-03-28 12:03	\$6,200	0.10888915	3Gjdrw	Wallet 4
2022-03-29 11:20	\$14,800	0.2602784	bc1qhl	Wallet 3
2022-03-30 10:50	\$10,000	0.17670476	bc1qhl	Wallet 3
2022-03-31 10:32	\$15,000	0.26801695	bc1qhl	Wallet 3
2022-04-01 10:40	\$15,000	0.26820749	bc1qhl	Wallet 3
2022-04-02 10:44	\$15,000	0.2706255	bc1qhl	Wallet 3
2022-04-03 11:33	\$5,000	0.0180183	bc1qhl	Wallet 3
2022-04-08 10:27	\$15,000	0.28455892	bc1qhl	Wallet 3
2022-04-09 11:54	\$15,000	0.29449125	bc1qhl	Wallet 3
<b>TOTAL:</b>	\$118,800	2.34959885		

c. Between March 31, 2022 and April 9, 2022, S.W. conducted at least seven transactions with National Air of Texas, in which she purchased approximately 1.49403686 BTC for approximately \$70,120. S.W. sent this BTC to various wallet addresses, including approximately 1.21846883 BTC to Wallet 3 (\$55,000).

Transaction Date	Transaction Value [Bitcoin]	Receiving Wallet Address
2022-03-31 14:42	0.2712255	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-01 15:07	0.18141177	3GjdrwhS9o9xUn4cw9MJePqRbXZBTR44aU
2022-04-01 15:14	0.09026909	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-02 15:13	0.27082485	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-04 15:14	0.09415626	3GjdrwhS9o9xUn4cw9MJePqRbXZBTR44aU
2022-04-08 14:42	0.28995034	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
2022-04-09 17:29	0.29619905	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r
<b>TOTAL:</b>	1.49403686	

//

//



Transaction Date	Transaction Value [Fiat]	Transaction Value [Bitcoin]	Receiving Wallet Address [Truncated]	Moniker
2022-03-31 14:42	\$15,000	0.2712255	bc1qhl	Wallet 3
2022-04-01 15:07	\$10,000	0.18141177	3Gjdrw	Wallet 4
2022-04-01 15:14	\$5,000	0.09026909	bc1qhl	Wallet 3
2022-04-02 15:13	\$5,000	0.27082485	bc1qhl	Wallet 3
2022-04-04 15:14	\$5,120	0.09415626	3Gjdrw	Wallet 4
2022-04-08 14:42	\$15,000	0.28995034	bc1qhl	Wallet 3
2022-04-09 17:29	\$15,000	0.29619905	bc1qhl	Wallet 3
<b>TOTAL:</b>	\$118,800	1.49403686		

#### ***Victim 4***

82. Victim 4 also reported being a victim of a BEC wire fraud scheme with losses totaling approximately \$302,683.25. Funds defrauded from Victim 4 have also been traced to conspirators involved in this BEC wire fraud scheme and to the Subject Wallet in the Subject Account.

#### ***L.S.***

83. On or about November 17, 2022, based on fraudulent wire instructions, Victim 4 wired \$302,683.25 to a Bank of America account ending in -4988. The receiving account is held in the name of [L.S.], doing business as Payoff Service Account (BOA Account 5).

a. Prior to receiving the wire from Victim 4, BOA Account 5 had a balance of \$100.

b. Other than this wire and reward payments totaling \$12.82, BOA Account 5 received no other deposits in November 2022.

c. At the close of the statement period, November 29, 2022, BOA Account 5 had a balance of \$100.25.

84. After the wire from Victim 4 was deposited to BOA Account 5, L.S. made a series of financial transactions, depleting approximately \$297,666.25 from BOA Account 5. These transactions included cash withdrawals (\$60,000), wire transfers to



other L.S. financial accounts (\$193,848), and wire transfers to accounts held by co-conspirator K.D.W. (\$43,818.25):

- a. On or about November 21, 2022, L.S. withdrew cash of \$10,000.
- b. On or about November 21, 2022, L.S. withdrew cash of \$50,000.
- c. On or about November 22, 2022, L.S. conducted two wire transfers, totaling \$150,000, from BOA Account 5 to Advantis Credit Union account ending in x3002, in the name of L.S. (ACU Account 1). The Balance on ACU Account 1 prior to these wire transfers was \$24,057.78.
- d. A few days later, on or about November 25, 2022, L.S. wired \$150,000 to a United Community Bank account ending in x4746, held in the name of [K.D.W.] Payoff Account Service (UCB Account 1).
- e. On or about November 29, 2022, L.S. wired \$48,848.00 to ACU Account 1. L.S. deposited an Advantis Credit Union cashier's check in the same amount and payable to L.S. to BOA Account 5 on or about December 1, 2022.
- f. On or about December 14, 2022, L.S. wired \$43,818.25 to K.D.W.'s UCB Account 1.

**K.D.W.**

85. K.D.W. received deposits into UCB Account 1 of approximately \$193,818.25 of funds transferred from L.S. accounts.

Date	Amount	Sending Account	Destination Moniker	Destination Account Number
11-25-2022	\$150,000.00	ACU Account 1	UCB Account 1	UCB-4746
12-14-2022	\$43,818.25	BOA Account 5	UCB Account 1	UCB-4746
Total:	\$193,818.25			

Immediately prior to receiving the \$150,000 wire transfer from L.S. on November 25, 2022, UCB Account 1 had a balance of \$12.15. Immediately prior to receiving the \$43,818.25 transfer on December 14, 2022, UCB Account 1 had a balance of \$2.15.

86. K.D.W. subsequently sent wire transfers totaling approximately \$192,000 from his accounts at United Community Bank to his account at Coinbase, for the purchase of virtual currency. Some of this virtual currency has been traced to the Subject Wallet in the Subject Account from which the Subject Cryptocurrency was seized.

a. On or about November 25, 2022, K.D.W. transferred \$150,000 to another United Community Bank in his name, ending in -4754 (UCB Account 2). Immediately prior to this transfer, UCB Account 2 had a balance of \$7.26.

b. On or about November 25, 2022, K.D.W. wired \$148,500 from UCB Account 2 to his account at Coinbase, a cryptocurrency exchange. Coinbase records reflect that on or about November 25, 2022, K.D.W. purchased 8.77 BTC, which was deposited to Bitcoin wallet address bc1qrrzml7jzqvr5pet8eatjnva0h7z58sux3cuspy (truncated, “bc1qrr”).

c. On or about December 14, 2022, K.D.W. wired \$43,500 from UCB Account 1 to his account at Coinbase.

(1) Coinbase records show that on or about December 14, 2022, K.D.W. purchased .86 BTC. The subsequent transaction shows .86 BTC was sent to Bitcoin wallet address bc1qw3uejwldxdf68pccunhdqt5y458z8h8sjaav35 (truncated, “bc1qw3”).

(2) Coinbase records show that on or about December 14, 2022, K.D.W. purchased .93 BTC. The subsequent transaction shows .93 BTC was sent to Bitcoin wallet address bc1q7etpnsfwfutadughlnf3lpd4ymm9vyksfn7mwrz (truncated, “bc1q7e”).

87. Blockchain analysis shows the BTC K.D.W. sent to the three wallet addresses identified above was transferred through a series of different wallets before being combined with other deposits on December 16, 2022, when a total of 10.344 BTC was sent to the Subject Wallet in the Subject Account. Approximately 8.88 BTC of this



1           91. Between December 23 and 31, 2021, M.K. depleted JPMC Account 2 to a  
2 balance of \$53.45 by transferring funds to other accounts under her control and  
3 withdrawing funds in cash.

4           a. On December 23, 2021, M.K. made two cash withdrawals from  
5 JPMC Account 2, totaling \$18,000.

6           b. On December 23, 2021, M.K. wired \$50,000 from JPMC Account 2  
7 to a Bank of America account in the name of The Payoff Service LLC, with the  
8 description "Partial Split From Sale."

9           c. On December 23, 2021, M.K. wired \$50,000 from JPMC Account 2  
10 to a Bank of the West account ending in x3405, in the name of M.K. (BOTW Account 1).  
11 Immediately prior to the deposit of this wire from JPMC Account 2, the balance on  
12 BOTW Account 1 was \$1,213.05.

13           (1) On the same day, M.K. wired \$10,000 from BOTW Account  
14 1 to a Bank of the West account ending in x3447, in the name of M.K. (BOTW Account  
15 2) and made a cash withdrawal in the amount of \$5,000.

16           (2) The following day, December 24, 2021, M.K. made a cash  
17 withdrawal from BOTW Account 1 of \$5,000 and withdrew an additional \$500 using an  
18 ATM.

19           d. On December 23, 2021, M.K. wired \$50,000 from JPMC Account 2  
20 to a Bank of America account in the name of The Payoff Service LLC.

21           e. On December 24, 2021, M.K. wired \$50,000 from JPMC Account 2  
22 to a Bank of America account in the name of The Payoff Service LLC, with the  
23 description "Split from Sale Remainder."

24           f. On December 28, 2021, M.K. made a cash withdrawal from JPMC  
25 Account 2 of \$10,000.

26           g. On December 29, 2021, M.K. made a cash withdrawal from JPMC  
27 Account 2 of \$5,000.

f. On December 31, 2021, M.K. transferred \$8,000 to an account ending x4935.

92. Bitcoin Depot records show that between December 23, 2021 and December 25, 2021, M.K. deposited \$35,000 in cash into Bitcoin Depot ATMs. A summary of those deposits appears in the table below:

Transaction Date	Transaction Value [Fiat]	Transaction Value [Bitcoin]	Transaction Bitcoin Address
12/23/2021	\$15,000.00	0.24602331	bc1q84eklysc2659p6cqhyfv8008ur88whq6nqp4tl
12/24/2021	\$5,000.00	0.08144616	bc1q84eklysc2659p6cqhyfv8008ur88whq6nqp4tl
12/25/2021	\$15,000.00	0.24738509	bc1q84eklysc2659p6cqhyfv8008ur88whq6nqp4tl

93. Between December 23, 2021 and December 25, 2021, wallet address bc1q84eklysc2659p6cqhyfv8008ur88whq6nqp4tl (truncated as “bc1q84”) received approximately 0.57 BTC from these three transactions.

94. Blockchain analysis shows that on or about December 28, 2021, 0.24601818 BTC was sent from wallet address “bc1q84” to wallet address bc1qfn979l84przccp6r9v302u48emglu20nrwh49 (truncated as “bc1qfn”). This BTC was further traced through a series of additional wallet addresses (nine total), a process known as a “peel chain”, a commonly used method to launder funds.

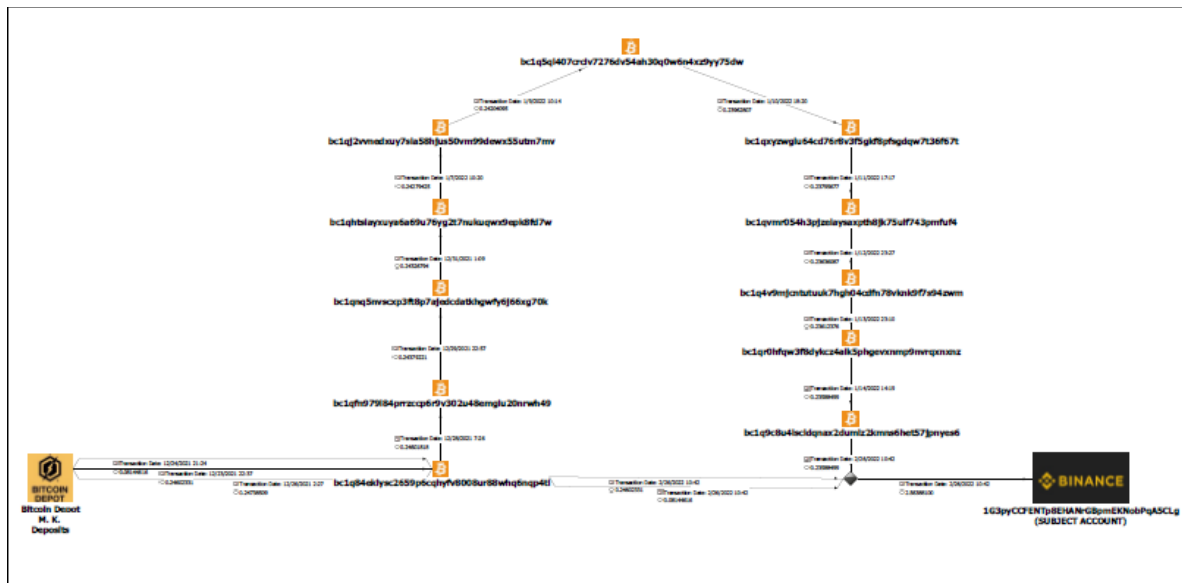
95. On or about February 26, 2022, the traced BTC was combined with other BTC deposits and a total of 2.56 BTC was sent to the Subject Wallet at the Subject Account. Approximately 0.56 BTC of this transaction is proceeds of, or derived from proceeds of, the wire fraud scheme and traceable to funds defrauded from Victim 5.

/

//

//

96. A visual representation of this tracing is provided below and is attached at Exhibit C:



97. The table below reflects the final transactions depositing the traced fraud proceeds from Victims 2 – 5 into the Subject Wallet:

Date and Time (UTC)	From	To	BTC Amount
2/26/2022 10:42:23	bc1q84eklysc2659p6cqhyfv8008ur88whq6nqp4tl	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.24602331
2/26/2022 10:42:23	bc1q84eklysc2659p6cqhyfv8008ur88whq6nqp4tl	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.08144616
2/26/2022 10:42:23	bc1q9c8u4lscldqnx2dumlz2kmns6het57jpnys6	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.23588499
3/16/2022 22:21:02	bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.0018947
3/16/2022 22:21:02	bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.09633957
3/16/2022 22:21:02	bc1q9nygzf9hghasdlqfzluu8a8kucwz0llhlt8wh	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.31649687
3/28/2022 23:36:39	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.00332022
3/28/2022 23:36:39	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.28358918
3/28/2022 23:36:39	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.11853435
3/28/2022 23:36:39	bc1qm3h49m0mdzrda0rwdly8vh04zv4wrt68zahe3	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.26297146
4/1/2022 22:57:58	bc1qhlzdc2xzp3xsdryg9jhzengya8j6kx7w4tsd3r	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.17502947
12/16/2022 18:03:56	bc1qea34l2ltafdxgpnvrh93f673qrlwzm7mxl2p5n	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.791292
12/16/2022 18:03:56	bc1qq0quwwz5hsun3knadmrgymxanzqgum7x2xwth	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	0.38714222
12/16/2022 18:03:56	bc1q57e8k5t7gfddcgg5n563mryav3lj0stj4nn7zp	1G3pyCCFENTp8EHANrGBpmEKNobPqA5CLg	7.71044545

1  
2 98. For each of the transactions, the victim funds were traced on the blockchain  
3 through a series of transfers between cryptocurrency addresses, known as “hops,” to their  
4 arrival in the Subject Wallet at the Subject Account.

5 99. Based on blockchain information, USSS investigators confirmed the  
6 transferring, purchasing, and exchange of the fraud proceeds through the blockchain (*i.e.*,  
7 the public ledger or record of all transfers) to the cryptocurrency and wallets identified in  
8 this Complaint. The blockchains for these cryptocurrencies revealed the date and time of  
9 the transactions involved, the originating public addresses for each transaction, the  
10 destination public addresses for each transaction, the amount of cryptocurrency  
11 transferred for each transaction, and the transaction hash (an identification number  
12 uniquely associated with that particular transaction that becomes part of the blockchain  
13 going forward). Based on this information, each transfer and exchange has been  
14 confirmed in the blockchain. Using publicly available blockchain explorers, USS  
15 investigators have traced fraudulently obtained funds from four identified victims of this  
16 BEC wire scheme to the Subject Wallet at the Subject Account.

17 100. The USSS’s investigation determined that the majority of the fraudulent  
18 transfers were sent through a series of virtual currency wallet addresses before ultimately  
19 being deposited into the Subject Wallet in the Subject Account at Binance. In response to  
20 a request for information, Binance provided account records for one user whose account  
21 was directly involved in the receipt of funds linked to multiple victims of the BEC wire  
22 fraud scheme described above.

23 101. On or about October 2, 2023, the USSS executed a properly authorized  
24 federal search warrant on the Subject Account and directed Binance to place the contents  
25 of the Subject Account – the Defendant Cryptocurrency – in a USSS maintained virtual  
26 currency wallet.

27 //



**X. CLAIM FOR RELIEF**

102. As required by Supplemental Rule G(2)(f), the facts set forth in this Verified Complaint support a reasonable belief that the United States will be able to meet its burden of proof at trial. More specifically, there is probable cause to believe that the Defendant Cryptocurrency is forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C) because it constitutes or is derived from proceeds of Wire Fraud, in violation of 18 U.S.C. § 1343 and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349, and pursuant to 18 U.S.C. § 981(a)(1)(A) because it is property involved in Money Laundering and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. §§ 1956 and 1957.

//

//

//

//

//

//

//

//

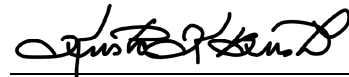
//

WHEREFORE, the United States respectfully requests:

1. A warrant be issued for the arrest of the Defendant Cryptocurrency;
2. Due notice be given to all interested parties to appear and show cause why the Defendant Cryptocurrency should not be forfeited;
3. Judgment be entered declaring the Defendant Cryptocurrency, any derivative cryptocurrency, and any interest to be condemned and forfeited to the United States for disposition according to law; and,
4. The United States be granted such other and further relief as this Court may deem just and proper.

DATED this 29th day of December, 2023.

Respectfully submitted,  
TESSA M. GORMAN  
Acting United States Attorney



---

KRISTA K. BUSH  
Assistant United States Attorney  
United States Attorney's Office  
700 Stewart Street, Suite 5220  
Seattle, Washington 98101  
Phone: (206) 553-2242  
Fax: (206) 553-6934  
[Krista.Bush@usdoj.gov](mailto:Krista.Bush@usdoj.gov)

**VERIFICATION**

I, Paul Vanderwulp, I am a Special Agent (“SA”) with the United States Secret Service (“USSS”) and have been so employed since November 2021. The USSS is the primary investigative agency charged with safeguarding the payment and financial systems of the United States. I am currently assigned to the Seattle Field Office as a member of the Cyber Fraud Task Force.

In my capacity as a Special Agent, I attended and completed the 21-week, 840 hour, USSS Special Agent Training Course at the James J. Rowley Training Center (RTC) located in Beltsville, Maryland. This program included comprehensive, formalized instruction in, among other things: fraud investigations, counterfeit identification and detection, familiarization with United States’ fraud and counterfeit laws, financial investigations and money laundering, identification and seizure of assets, physical and electronic surveillance, and undercover operations. I completed the 59 days and over 470-hour Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC).

In January 2023 I completed 120 hours at the Basic Network Intrusion Responder Training (BNITRO) at RTC in Beltsville, MD. The focus of the training was to establish a foundation for Digital Forensic Network Intrusion – Network Response (DFIR-NI) for common schemes and illicit activity including but not limited to, Business Email Compromise (BEC), Ransomware and Point of Sale (POS) system breaches. I have completed 40 hours at the National Computer Forensic Institute (NCFI) which included cyber investigations with computers and phones. NCFI also consisted of investigative procedures, law enforcement procedures, cybercrime training, and mobile device/data analysis as it relates to criminal investigations.

//

//

1 During my time in federal law enforcement, I have been trained in criminal  
2 investigations. This training has involved investigation into the unlawful takeover of  
3 financial accounts, business email compromise schemes, network intrusions, counterfeit  
4 currency investigations, and protective intelligence investigations.

5 In 2017, I attended a 40-hour class at FLETC entitled, "Money Laundering and  
6 Asset Forfeiture". In 2016, I attended the 120 hour Washington State Patrol Detective  
7 Basic course located in Shelton, WA. In September 2013 I was hired as an officer for the  
8 Washington State Liquor and Cannabis Board and in December of 2014 graduated the  
9 720-hour Basic Law Enforcement Academy (BLEA) at the Criminal Justice Training  
10 Center (CJTC) in Burien, WA.

11 I graduated in May 2012 from Azusa Pacific University with a Bachelor of Arts  
12 (B.A) in Business Administration. In May 2012 I began employment with Nordstrom as a  
13 Loss Prevention Agent.

14 My duties included internal, external and process loss management. This included  
15 training on theft, robbery, device fraud, identity theft, organized retail theft (ORT) and  
16 other Revised Code of Washington (RCW) criminal statutes.

17 I am an investigating or law enforcement officer of the United States within the  
18 meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct  
19 investigations and to make arrests for federal offenses. I furnished the investigative facts  
20 contained in the foregoing Verified Complaint for Forfeiture *In Rem*. The investigative  
21 facts are based on personal knowledge I obtained from my involvement in the underlying

22 //

24 //

26 //

1 investigation, my review of the relevant investigative material, other federal agencies and  
2 law enforcement officers involved in the investigation, other reliable official Government  
3 sources, and my own training and experience.

4 I hereby verify and declare, under penalty of perjury pursuant to 28 U.S.C. § 1746,  
5 that I have read the foregoing Verified Complaint for Forfeiture *In Rem*, that I know its  
6 contents, and that the facts it contains are true and correct to the best of my knowledge.

7  
8 Executed this 29<sup>th</sup> day of December, 2023.

9  
10  
11 

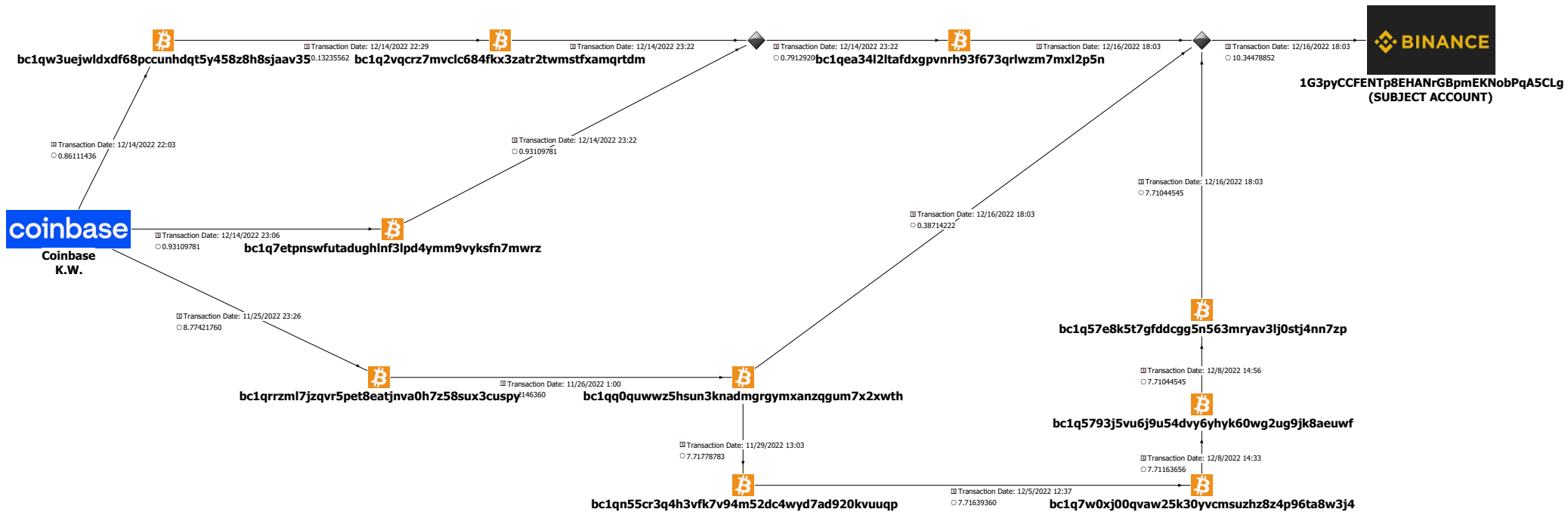
12 PAUL VANDERWULP  
13 Special Agent  
14 United States Secret Service  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

# **EXHIBIT A**

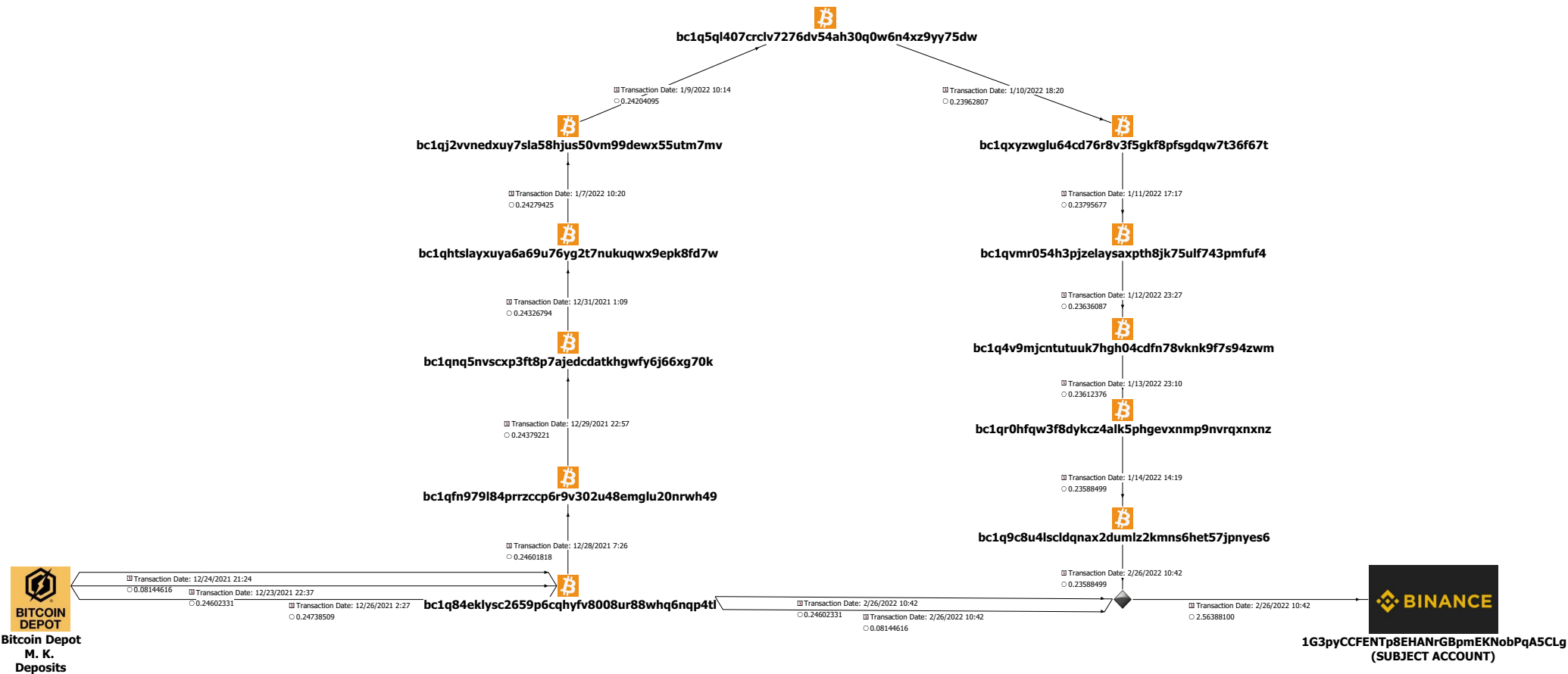




# **EXHIBIT B**



# **EXHIBIT C**



# **EXHIBIT D**

## FLOW OF FUNDS BEC TO BINANCE

